

AIR WAR COLLEGE

AIR UNIVERSITY

CHEMICAL/BIOLOGICAL-CAPABLE RPA THREATS  
AND NATIONAL SECURITY IMPLICATIONS

by

Jason A. Lay, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Albert Mauroni

7 February 2016

## **DISCLAIMER**

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.



## **Biography**

Lt Col Jason Lay entered the Air Force in 1994, after graduating from the University of Portland with a bachelor's degree in mechanical engineering. Following four years of active duty as an acquisitions officer, he transitioned his service in 1998, to the Oregon Air National Guard with the 142<sup>nd</sup> Civil Engineer Squadron, Portland, Oregon. There he served as the engineering flight officer, operations officer, and he took command of the squadron in 2013. Lt Col Lay's deployment experience includes Hungary, Bosnia-Herzegovina, Saudi Arabia, and two tours in Afghanistan where he commanded the 455<sup>th</sup> Expeditionary Civil Engineer Squadron at Bagram Airfield in 2014. He is currently assigned to the Air War College, Air University, Maxwell AFB, AL.



## **Abstract**

The technological landscape of the 21<sup>st</sup> century is evolving at an ever-increasing pace. Autonomous remotely piloted aircrafts (RPAs) continue to become increasingly sophisticated in size, range, and capability. In addition, emerging micro and nano-technologies are exposing new potential threats in chemical and biological warfare (CBW) not possible just a few years earlier, opening the door to previously unthinkable potentials. Further still, existing chemical and biological treaties, widely adopted around the globe, do not adequately address these prospective and evolving threats, leaving room for potential exploitation by foreign players. The defense posture of the United States is not adequately prepared for the combined threat of today's cutting-edge advancements.

Future national defense efforts must envelop critical vulnerabilities posed by emerging technologies in order to protect Americans and deter adversarial use of chemical and biological-capable RPAs. In order to stay ahead of these growing threats and to thwart would-be abusers of advanced technologies, the U.S. Government (USG) must consider changes to how it defends its own airspace. Both active and passive measures of defense with multi-dimensional capabilities are the best approach to achieving this objective. Additionally, modernization of individual protective equipment to align with the current operational environment, and modification to the international chemical and biological conventions must occur to address existing coverage gaps in an effort to keep pace with the ongoing advances of science and technology.

The swift and proper implementation of the proposed recommendations will result in the improved defense and protection of American forces from an emerging method of attack.

Where we are with UAVs is about where we were with Bi-planes just after WWI. We are at the very early stages of realizing what the potential of UAVs are.<sup>1</sup>

David A Deptula, Lt. General, USAF (Ret.)

## **Introduction**

The technological landscape of the 21<sup>st</sup> century is evolving at an ever-increasing pace. Autonomous remotely piloted aircrafts (RPAs) continue to become increasingly sophisticated in size, range, and capability. While research and development continues to progress, the availability and utility of RPAs continue to grow among both civilians and the military, making them a prime candidate for use in irregular warfare by both state and non-state actors. The U.S. Air Force (USAF) predicts that one third of its military and attack fighter planes will be unmanned within the next ten years.<sup>2</sup> In addition, emerging micro and nano-technologies are exposing new potential threats in chemical and biological warfare (CBW) not possible just a few years earlier, opening the door to previously unthinkable potentials. Further still, existing chemical and biological treaties, widely adopted around the globe, do not adequately address these prospective and evolving threats, leaving room for potential exploitation by foreign players. The defense posture of the United States is not adequately prepared for the combined threat of today's cutting-edge advancements. The U. S. Government (USG) should consider addressing the growing risks introduced by emerging technologies that are generating new threats to U.S. national security not thwarted by present-day defense capabilities and international treaties. Future national defense efforts must envelop critical vulnerabilities posed by emerging technologies in order to protect Americans and deter adversarial use of chemical and biological-capable RPAs.

This paper will start by highlighting many recent advancements contributing to the technological developments of RPA vehicles. Second, it will review the existing defense capabilities of U.S. forces and installations with respect to potential vulnerabilities. Third, it will expose viable gaps contained in the Chemical Weapons Convention (CWC) and Biological Weapons Convention (BWC) concerning 21<sup>st</sup> century capabilities. Finally, the paper will conclude with analysis and recommended actions to address some of the presented concerns.

### **Cause for Alarm**

In January 2015, a lone individual flew a small quad-copter onto the grounds of the White House. While the event was deemed an accident, it still resonates with implications of what might be possible by someone with hostile intentions. Do these small RPAs pose a realistic threat? If so, what are they capable of and how do you defend against them? According to Dr. Steven Huybrechts of Applied Minds, LLC, “The threat to National Security is already here [and] we’ll have to figure out something quite soon to deal with it.”<sup>3</sup> As a primer to the following discussion, first consider this hypothetical scenario:

On an October Tuesday afternoon, just outside the view of local Security Forces personnel near Joint Base Anacostia-Bolling, a lone terrorist walks along the treed fence line. Behind him, he pulls a wheeled footlocker through the grass. He stops beneath a large tree, covers the plastic case with camouflage netting, and then hides the package within the tree. Glancing around to be sure he is not being watched, he flips the master switch and walks away.

A few minutes later, a small drone emerges from inside the footlocker; the miniature aircraft is only a few inches wide and even smaller in height. The drone

hovers clear of the tree then climbs toward the tall perimeter fence, easily passing over the triple-strand barbed wire. It is now on the base.

Guided by a combination of GPS, two-way radio communication and an on-board inertial navigation unit, the drone travels above the rooftops of base facilities and vectors toward the large Defense Intelligence Agency (DIA) building just inside the main gate. Busy pedestrians walking below do not even notice the faint sound or small silhouette traversing the sky.

Back at the footlocker, additional drones emerge from the box and proceed onto the base, twenty in all. Five head to the DIA, while others depart for the Command Post and general officer housing. Upon arrival, each drone surveys its surroundings via onboard camera and transmits real-time data and imagery back to the central computer. The terrorist, miles away on a Metro bus, watches the events unfold from his smartphone.

The drones at the DIA swarm onto the roof and gather near the large air handler intakes. In unison, they excrete several clouds of atomized Sarin liquid into the ventilation system exposing hundreds of unsuspecting workers inside the facility.

Arriving at the general's housing, the other drones disperse throughout the neighborhood and settle out of sight near doors and walkways. They transition into 'sleep mode' while their proximity scanner waits to detect approaching activity. When that occurs, they will burst from hiding and spray their lethal venom right in the face of an unsuspecting victim.

By this time, the DIA building is undergoing a mass exodus and the base has initiated total lockdown at FPCON DELTA, MOPP level 4. The CAT and EOC are activated and key personnel are scurrying to their response locations while the remaining base population takes cover in-place under blaring wavering sirens. As responding Airmen arrive outside the Command Post dressed in their MOPP gear, the nearby drones analyze IR imaging to identify human heat signatures, orientation, speed and direction of incoming personnel. The Airmen's only defenses are designed against a passive airborne threat; however, these drones each employ a single hypodermic dart laced with a bioengineered virus—the needle easily penetrates their protective suits and into the skin.

It will take days before the tension is relieved and leaders are able to contemplate how America was once again surprised by a lethal attack on its own soil. Meanwhile, all the drones return to the footlocker off base and the terrorist, avoiding discovery, retrieves his deadly package without leaving a trace.

This chilling scenario may seem like a Hollywood-style fantasy; however, this threat is entirely plausible with existing and developing technologies. Mr. Clint Hope, Chief Scientist at Applied Minds, LLC—an innovative, technical solutions company based in Burbank, California—says, “Swarms of autonomous inertially guided drones with speeds up to 400 mph, extended range, and enough payload to deliver traditional and non-traditional threats already exist and we should be prepared for them targeting US installations.”

### **Current and Emerging Technologies**

Traditionally, the development, production, and employment of chemical or biological weapons required a large industrial footprint and sophisticated delivery systems only available to

state actors. However, recent advances in technology allow for the precision distribution of CBW without the need for huge stockpiles or the randomness of large plume deliveries.

Technology, in effect, is beginning to overcome these prohibitive obstacles and open doors of possibility to those who wish to do harm by using chemical and biological weapons.

The review of current and emerging technologies will focus on several categories of application. First, we will deal with RPA technology by examining the elements that make it a reliable and effective platform. The next topics will include a look at the supporting technologies and factors complimenting the continued sophistication of future RPAs, such as manufacturing technology and dedicated research. Finally, we will examine nanotechnology and bioengineering advances and their impact on future chemical and biological weapons.

While RPA technology has existed in one form or another for decades, recent key advancements in micro-RPAs have synergized to improve their performance and reliability. These ingredients combine to make this technological leap possible such as advanced microprocessors and dedicated research. Microprocessors are the brain of all computing devices. They are the integrated circuit chips that interpret software programming. Since the dawn of the computer age, microprocessors have continued to shrink in both size and cost, while simultaneously growing in performance, capacity, and speed. Their widespread application in a multitude of products around the world has contributed to increased availability. Currently, a credit card-sized microprocessor, which is 28 times faster than an Intel 486 processor and possessing four hundred times more memory, is now commercially available for less than \$35.<sup>4</sup> Ongoing research contributes to the evolution and overall progress of RPA development. Dozens of agencies are devoting hundreds of millions of dollars to RPA research and

development. In 2016 alone, the U.S. Air Force projects to spend approximately \$123M on unmanned aerial vehicles and RPA research.<sup>5</sup>

Several supporting technologies are also contributing with no less significant impacts. Additive manufacturing (3D printing) is changing the way products are constructed. While 3D printing has been around since the 1980's, like many new developments, it took decades to mature and become a readily available and affordable process.<sup>6</sup> Today, commercially available 3D printers sell for less than \$400. The process of 3D printing allows for rapid production of very complex components that used to take large amounts of time and money. Additive manufacturing advances micro-RPA technology due to its small, lightweight characteristics. An additional benefit of 3D printing allows a person on one side of the world to print a physical part on the other side of the world with the touch of a button. This capability is unique to additive manufacturing and represents a significant shift in the proliferation of fabrication processes.

Advancements in manufacturing technology continue to progress as emerging new concepts are demonstrated in the lab. Researchers at Massachusetts Institute of Technology are now developing 4D manufacturing, which adds the new dimension of self-assembly to the manufacturing process.<sup>7</sup> Efforts are also underway to expand the types of materials adaptable for printing. Besides plastic and some metals, researchers have developed capabilities to print functional materials, which include conductive and non-conductive components. This achievement enables the printing of electrical circuitry directly on three-dimensional parts during fabrication; future projected enhancements include the ability to print resistors, diodes, and other electrical components.<sup>8</sup> Enhancements such as these have immediate application to the production of small or micro-sized RPAs. Continued future improvements could potentially develop the ability to print an assembled, full-functioning RPA without any human intervention.

The technical capabilities described above combine for the overall enrichment of RPA development. In addition, future advancements generated from dedicated research are also promising. New means of achieving lift and propulsion for small aerial vehicles are currently in development. In 2011, Defense Advanced Research Projects Agency (DARPA) made public the achievement of a flapping-wing RPA called “Hummingbird.”<sup>9</sup> This small device, with a six-inch wingspan, is capable of vertical takeoff and landing, as well as controlled flight in all directions. It does not use rotational motion for lift; therefore, it does not require a tail section, elevator, vertical stabilizer, or counter torque propeller as necessary with most common aircraft designs. Finally, in 2014, a team working at Harvard University successfully achieved flight with their nano-RPA device called “RoboBee.”<sup>10</sup> The insect-like vehicle has a wingspan of only three centimeters and represents the smallest man-made device (modeled after an insect) to ever achieve flight. Current progress requires the tiny robotic insect to be tethered; however, future designs are working toward autonomous, untethered versions that communicate with an entire “hive” of other RoboBees. These recent accomplishments are furthering the capabilities of micro-RPAs, yet such improvements could also allow for exploitation when combined with advances in other fields of study. Specifically, nanotechnology and bioengineering are making strides into previously uncharted territories. While their development has beneficial intentions, the potential for misuse remains present and could introduce unforeseen utility in CBW employment.

Nanotechnology and Bioengineering are advanced scientific fields of study with positive contributions in multiple disciplines such as information technology, healthcare, and materials science. While primarily conducted under laboratory conditions, their contributions to the field of chemistry and biology have many practical applications. Nanotechnology is the manipulation

of the physical makeup and structure of materials at the molecular level.<sup>11</sup> It enables direct control of atomic building blocks for influence over material properties. This level of control leads to the development of non-naturally occurring compounds such as lighter and stronger materials. With regard to CBW, it also lends itself to the potential development and production of new chemical compounds without historically large industrial processes. This capability could change the approach to manufacturing chemical weapons, enabling their availability to small-scale actors.

Similar to nanotechnology, bioengineering is capable of creating new types of microbial or biological organisms through controlled manipulation of biological compounds. In 2014, a researcher at the University of Wisconsin reportedly constructed a new version of the flu virus from wild-avian-flu strain genes. This new virus proved capable of spreading from one host to another and had more infectious properties than the original virus.<sup>12</sup>

Research in these fields have yielded the creation of nanobots—tiny machines or organisms that perform medical tasks internally within the body or bloodstream. Nanobots are either entirely constructed of DNA proteins, which are genetically programmed to perform specific functions, or they can be made of inorganic materials capable of navigating through the body with magnetic motive propulsion able to deliver medication to needed tissues.<sup>13</sup> Specific developments like these could potentially be adapted for adversarial uses in CBW development and employment.

### **Defensive Capabilities**

In consideration of the evolving threats imposed by technological advances, it is necessary to evaluate the specific defense capabilities of U.S. forces and facilities concerning their capacity to prevent, detect, and defend against future attack from CBW-capable RPAs.

This review will specifically evaluate Anti-Access/Area Denial (A2/AD), CBRN Detection, and Individual Protective Equipment (IPE).

Typical discussions of A2/AD focus on the ability of U.S. forces to overcome the defenses of an adversary. However, in this context we are referring to the ability of U.S. military forces to impose A2/AD against and adversarial use of its own airspace. A2/AD relies upon two major features, 1) the ability to detect the presence of an adversary, and 2) the ability to deny adversarial use of a given region of airspace. Therefore, we must answer two main questions: Do we possess the ability to detect micro-RPAs, and are we able to prevent their use in a given airspace?

With regard to detection, the capability definitely exists. Airspace detection and radar equipment are technologically capable of locating insect-sized flying objects. However, the difficulty lies within the capacity to determine whether a detected object is an RPA or whether it is an insect or bird. Plausibly this distinction is achievable with human or computational evaluations; however, the ability to detect and evaluate a small object in a large open field is not the same as being able to distinguish the same object operating in and amongst several buildings and trees. Additionally, RPA control programming could mimic the flight characteristics of birds in order to fool detectors, analytic algorithms, and even humans. As long as low-flying micro-RPAs have the ability to blend in with birds and insects, the effort of detection will remain prohibitively difficult.

Assuming the challenges of detection are solvable, the next challenge to face is that of denial. Traditional airspace denial employs a combination of surface to air missiles and air-to-air combat aircraft at great standoff distances from critical assets. However, these defensive measures would prove ineffective against any number of micro-RPAs. Current capabilities

specialize in defeating large aircraft with precision kinetic weapons. In effect, the introduction of RPAs into U.S. airspace defense reveals a significant gap in the air superiority model. The current threshold of U.S. capabilities does not extend low enough to address these threats with traditional methods.

In practice, Security Forces (SF) personnel on the ground conduct the primary A2/AD effort at homeland USAF installations. SF Airmen protect base perimeters and airfields to prevent unauthorized access. While overall base defense is their responsibility, their security procedures do not include provisions for defending the airspace of the installation. Existing perimeter defenses are largely passive—consisting of fencing and barbed wire aimed at denial of personnel and vehicles. These defenses present little challenge for RPAs operating just ten feet above the ground providing complete and largely undetected access of an entire base complex. If an influx of micro-RPAs were to breach a base perimeter, local wing leadership would look to SF personnel as the primary means of defense and quickly realize that they are ill-equipped to respond to such a situation. It is evident that U.S. installations are not prepared to project A2/AD against the emerging RPA threat.

Existing CBRN detection equipment uses methods optimized for traditional CBW employment on the battlefield. Multiple detection stations distributed throughout a base act as a network of nodes for determining the presence of plumes of CBW over large areas. However, as demonstrated in the opening scenario, the use of RPA-distributed chemical or biological agents at precise locations would counter the value of these detectors. Their data would offer little certainty in determining affected or unaffected areas rendering serious limitations to their usefulness.

In the event of a CBW event, USAF personnel are trained to don the Joint Service Lightweight Integrated Suit Technology (JSLIST) IPE ensemble and M50 Joint Service General Purpose Mask. These items are effective for operations of short durational exposure in chemical and biological affected environments. The primary defenses provided by this ensemble are the air filtering and prevention of skin contact. This defense method is effective against a passive fallout cloud; however, simple aggressive measures could easily overcome the effectiveness of the CBRN IPE ensemble. The thin rubber gloves are a primary target of weakness against any kind of penetrating projectile, which are conceivably dispersible from a micro-RPA. Additionally, the suit itself is easily penetrable and is consequently susceptible to exploitation as well. Lastly, the critical value of the M50 mask makes it a natural target. Disruption of the mask seal, puncture of the lens, or saturation of the filter intake are all significant vulnerabilities. It is therefore plausible that current MOPP postures are not an adequate defense mechanism to oppose a technologically-advanced RPA with CBW capabilities.

Finally, we will review the psychological impact potential of CBW. Throughout history, the employment of CBW has possessed the capability to evoke fear due to its perception as an inhumane tactic. This psychological reaction of fear is very powerful. Similarly, terrorism seeks to utilize fear over its adversaries in order to accomplish its strategic objectives, making full use of this powerful influence. Therefore, the combination of terrorism and CBW manifests an even greater dose of fear than either one individually. Even though there are only a few historical examples of terrorists utilizing CBW, it is worth recognizing the influence of this probable combination. Past limitations to access and employment of large stockpiles of CBW and complex delivery systems may have previously prevented terror groups from incorporating CBW; however, it is now conceivable that advancements such as RPA technology could

eventually overcome the resistive hurdles of these weapon-types and give rise to new methods of employment.

### **International Treaty Language**

With the constant progress of technological advances described above, is the language of the international Chemical Weapons Convention (CWC) and Biological Weapons Convention (BWC) still relevant for these current and emerging challenges? An evaluation of the CWC and BWC follows.

On the surface, the CWC appears to address the development, production, acquisition, stockpile, retention, transfer, use, and preparations of chemical weapons.<sup>14</sup> Likewise, the CWC definition of chemical weapons is broad enough to encompass unforeseen methods and equipment such as might be developed under future technologies. Further, the definition of “Toxic Chemical” in Article II, paragraph 2, includes a very broad scope, regardless of origin or production method; this would seem to be sufficiently protective as well.<sup>15</sup> However, upon further review, there appears to be an anomaly subject to exploitation with regard to incapacitants and riot control agents (RCAs).<sup>16</sup> Article I, paragraph 5, specifically states that RCAs will not be used for warfare, but this leaves other implemented uses of RCAs, such as for law enforcement purposes, not restricted by the CWC. This gap in coverage allows a signatory member of the CWC to develop, store, and use chemical RCAs for non-warfare purposes (e.g., internal security operations). In addition, the definition of RCAs in Article II, Paragraph 7, includes the phrase “disabling physical effects” of a temporary nature, which is difficult to distinguish from incapacitants. The CWC expressly covers temporary incapacitants as chemical weapons and prohibits their use; however, the definition of incapacitants is not clear in Article II and thereby allows for the possible misinterpretation of this element. While not directly related

to technological advancements, a small loophole such as this permits rogue actors the prospect to exploit the use of chemical weapons potentially without reprisal.

With regard to the BWC, it likewise is extremely thorough in addressing the breadth of definitions for microbial and biological agents.<sup>17</sup> In fact, it sufficiently covers the improper development or use of any bioengineered organisms or viruses that may emerge in future warfare. However, as identified above, the field of nanotechnology could conceivably advance to produce non-organic autonomous mechanisms designed for internal uses; these could have devastating and perhaps lethal results. This kind of weaponry, while not biological in nature, could produce similar effects as biological warfare agents. Since the structural makeup of these nanobots is not a microbial, a toxin, nor a biological agent, their development, production and employment are clearly outside the defined boundaries of the BWC. The emerging risks associated with this new technology present a completely new subject requiring further investigation for national and international policy decisions.

### **Analysis**

It is clear that recent scientific and technological advancements are introducing new potential threats, but what is the likelihood of these threats manifesting into real-world events from an adversary? Is it reasonable to expect a signatory foreign state would seek to take advantage of seemingly minute loopholes in the international chemical and biological conventions? And what techniques or procedures are likely to decrease U.S. vulnerability to such actions? These questions are not easy to answer; however, the following section attempts to address the latter by providing proposed recommendations.

The cataclysmic events of 9/11 unmistakably demonstrated that advanced technology (long-range aircraft) in the hands of just a few skilled terrorists is capable of imposing large-

scale, deadly and destructive effects on thousands of people, communities, and an entire nation. The attack on that day was arguably unexpected and few preventative measures were in place that could have stopped it from occurring. While future adversarial threats may continue to be unique and consequently elusive, efforts to identify and respond to remote-chance, emerging dangers should increase to an all-time high. While attempting to prevent every foreseeable threat can be an extremely costly proposal, it is imperative that as many threats as possible be identified to allow for compilation, analysis, and prioritization of each according to their merits. Identified threats should undergo thorough exploration and consideration in terms of their severity and potential. Likewise, counter-measures to impede their effects should be developed and assessed for practicality of implementation and effectiveness. This represents the best way to evaluate existing and impending dangers and to determine the appropriate measures of response.

### **Recommendations**

Despite the vast array of technological advances imposing new threats to U.S. national security, several options are available for consideration in order to minimize, reduce or possibly eliminate these threats.

In the area of RPA technology, it is highly recommended the USG stay on the leading edge of research and development. Dedicated research through agencies like DARPA, Defense Threat Reduction Agency, universities, and research grants will help ensure U.S. forces have the best technology available in the field of RPAs.

Enhancements in defense capabilities are a necessary consideration in order to address the growing threats imposed by RPAs. Specific recommendations include low-level radar detection at U.S. installations and high-profile facilities with the capability to distinguish

between, organic and inorganic objects and identify potential drone operation within a given airspace.

Along with enhanced detection capabilities, I recommend implementing both active and passive area denial methods for small, micro, and nano-size RPAs. A simple, low-tech, passive solution would protect facilities by installing netted or fenced cages to impose fixed standoff distances away from fresh-air intake vents.

A possible active defense method for neutralizing small RPAs is the use of a shotgun or similar weapon to thrust an array of projectiles at a target. However, depending on the environment, and especially near flying operations, shooting firearms into the air would impose serious drawbacks and concerns. High-tech sentry guns, such as the Phalanx Close-In Weapons System (CIWS) utilized by the U.S. Navy, provide autonomous computer-guided tracking and firing capable of destroying small and fast inbound enemy projectiles, rockets, and aircraft. Similar versions of this weapon system are in operation around active airfields and populated areas utilizing complex algorithms for detection and aiming to avoid unwanted damage to friendly or coalition assets. Targeting capabilities include detection of small profile objects measuring less than one meter in length and at velocities over 300 miles per hour. With a firing rate of three thousand rounds per minute and utilizing mid-air exploding projectiles in order to limit the range and potential for collateral damage, this system has a high potential for application in defending against an RPA threat. However, kinetic defensive measures are limited in their capacities for simultaneous effect. Systems like the CIWS can effectively only defend against a single target at a time and firearms require maintenance and reloading causing interruptions in defense capabilities. These drawbacks can be overcome by means of a network of multiple systems, which increases their overall capacity.

Other high-tech solutions capable for RPA defense include incapacitating directed energy, such as acoustic or microwave radiation; sensory overload devices to confuse or overwhelm RPA inputs causing disorientation; electronic or electromagnetic disruption; or lastly a defensive swarm of RPAs designed to target and destroy intruding RPAs of various size and capability. While these unconventional defensive methods require further testing and development, they offer the distinct advantage of having broad simultaneous effects over large areas and are capable of continuous operation without the delays imposed by kinetic defensive measures identified above.

Blighter Surveillance Systems, a British-based company, sells an Anti-UAV Defense System (AUDS) capable of detecting, tracking, and neutralizing unmanned aircraft systems. AUDS utilizes directional radio frequency (RF) inhibition to take down its objectives. While this might appear to be a viable defensive solution, the drawbacks to this system are rooted in its one-dimensional method of disruption. RF communication is a common control method for RPA operation; however, it is not the only process available. Unfortunately, the AUDS would prove ineffective against an advanced RPA equipped with on-board inertial navigation and not reliant upon outside signals for routing and control. Successful employment of RPA defensive measures will likely utilize multi-dimensional efforts capable of delivering a family of impedances to thwart unwanted RPA operations.

Additional recommendations include improvements to the protection of personnel in the CBRN environment. JSLIST ensemble upgrades could include anti-piercing membranes to resist targeted injections--glove materials require similar upgrades as well. A protective clip-on screen installed over the air intake of the M50 mask would prevent successful filter targeting intended to clog or overwhelm the wearer's breathing process. Modernization of IPE to include defensive

measures against active threats, as opposed to just passive, would allow for greater protection of personnel.

Lastly, I recommend the closure of loopholes identified in the international chemical and biological conventions. This will dispel ambiguity surrounding the use of chemical agents for non-warfare activities and provide definitive clarity on RCAs and incapacitants. Similarly, it will define and prohibit employment of inorganic objects, such as nanobots, within humans or animals capable of causing harmful or lethal effects. Alternatively, the United Nations Convention on Certain Conventional Weapons, which already deals with lethal autonomous weapons systems, is another potential mechanism to encompass the prohibition of inorganic, biological devices. Since many countries have already ratified these conventions, the best mechanism for change may be through annexation of additional protocols at an upcoming UN review conference (RevCon). These revisions will likely take a great deal of time and effort to implement, which is why I recommend them for immediate action.

## **Conclusion**

The continually evolving landscape of technology is producing new threats to U.S. national security. This process of change allows for the emergence of adversarial capabilities only made possible within the past few years. Among them, and of highest concern, is the employment of CBW-capable RPAs. The expansive and ever-pressing force of technological progress is unstoppable; therefore, the best response is to observe and acknowledge the vulnerabilities it exposes and then take appropriate action to close the gaps.

In order to stay ahead of these growing threats and to thwart would-be abusers of advanced technologies, the USG must consider changes to how it defends its own airspace. The longstanding dominance of U.S. air superiority is only sustainable as long as key leadership

remains brave enough to support the continual evaluation of its weaknesses. Both active and passive measures of defense with multi-dimensional capabilities are the best approach to achieving this objective. However, defense of the airspace is not enough; we should also modernize the protection of personnel with advanced IPE improvements that address the current operational environment. And we must consider modifications to the international chemical and biological conventions to close existing gaps and keep pace with the ongoing advances of science and technology. No nation can afford to have a hole in their umbrella of legal protection.

As technology continues to advance, it will simultaneously introduce and expose new threats and vulnerabilities to US national security. The proper response is always a difficult task faced by national strategic leaders. One thing is certain; failure to respond to known threats is a never-ending gamble against time—eventually disaster will strike. However, swift and proper implementation of the recommendations presented above will result in the improved defense and protection of U.S. forces from this emerging danger.

## Notes

<sup>1</sup> Quoted in “Rise of the Drones,” *Nova*, directed by Peter Yost (Public Broadcast Service, 2013), <http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html>

<sup>2</sup> “Rise of the Drones,” *Nova*, directed by Peter Yost (Public Broadcast Service, 2013), <http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html>

<sup>3</sup> Dr. Steven Huybrechts (Applied Minds, LLC), interview by the author, 23 November 2015.

<sup>4</sup> “Raspberry Pi 2 Model B.” Raspberry Pi. Accessed 4 October 2015. <https://www.raspberrypi.org/products/raspberry-pi-2-model-b/>.

<sup>5</sup> “Drones in the Defense Budget.” Center for the Study of the Drone. Accessed 5 October 2015. <http://dronecenter.bard.edu/drones-in-the-defense-budget/>.

<sup>6</sup> “3D Printing History: The Free Beginner’s Guide.” 3D Printing Industry. Accessed 5 October 2015. <http://3dprintingindustry.com/3d-printing-basics-free-beginners-guide/history/>.

<sup>7</sup> “4D Printing: Multi-Material Shape Change.” Self Assembly Lab. Accessed 5 October 2015. <http://www.selfassemblylab.net/4DPrinting.php>.

<sup>8</sup> “Materials for 3D Electronics Printing.” Voxel8: 3D Electronics Printing. Accessed 8 October 2015. <http://www.voxel8.co/materials/>.

<sup>9</sup> “AeroVironment Develops World’s First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA.” Aero Vironment. Accessed 5 October 2015. [http://www.av-inc.com/resources/press\\_release/aerovironment\\_develops\\_worlds\\_first\\_fully\\_operational\\_life-size\\_hummingbird](http://www.av-inc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird).

<sup>10</sup> “Robobees.” Accessed 4 October 2015. <http://robobees.seas.harvard.edu/>.

<sup>11</sup> “Benefits and Applications | Nano.” Accessed 7 October 2015. <http://www.nano.gov/you/nanotechnology-benefits>.

<sup>12</sup> “Making Viruses in the Lab Deadlier and More Able to Spread: An Accident Waiting to Happen.” Bulletin of the Atomic Scientists. Accessed 6 October 2015. <http://thebulletin.org/making-viruses-lab-deadlier-and-more-able-spread-accident-waiting-happen7374>.

<sup>13</sup> Ackerman, Evan. “Robotic Micro-Scallops Can Swim Through Your Eyeballs,” November 4, 2014. <http://spectrum.ieee.org/autatome/robotics/medical-robots/robotic-microscallop-can-swim-through-your-eyeballs>.

<sup>14</sup> “Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction.” Accessed 5 October 2015. <http://disarmament.un.org/treaties/t/cwc/text>.

<sup>15</sup> Ibid.

<sup>16</sup> “Chemical Weapons Convention Fails to Address Key Issues - SciDev.Net.” Accessed 6 October 2015. <http://www.scidev.net/global/governance/news/chemical-weapons-convention-fails-to-address-key-issues.html>.

<sup>17</sup> “UNODA - The Biological Weapons Convention.” Accessed 6 October 2015. <http://www.un.org/disarmament/WMD/Bio/>.



## Bibliography

- “3D Printing History: The Free Beginner’s Guide.” 3D Printing Industry. Accessed 8 October 2015. <http://3dprintingindustry.com/3d-printing-basics-free-beginners-guide/history/>.
- Ackerman, Evan. “Robotic Micro-Scallops Can Swim Through Your Eyeballs,” November 4, 2014. <http://spectrum.ieee.org/automaton/robotics/medical-robots/robotic-microscallop-can-swim-through-your-eyeballs>.
- “Aircraft Insects’ Development - Information Center City of Science and Technology – Information Center of Science and Technology City.” Accessed 8 October 2015. <http://www.cesti.gov.vn/khong-gian-cong-nghe/may-bay-con-trung-phat-trien/content/view/7883/286/81/1.html>.
- “Benefits and Applications | Nano.” Accessed 8 October 2015. <http://www.nano.gov/you/nano-technology-benefits>.
- “Chemical Weapons Convention Fails to Address Key Issues - SciDev.Net.” Accessed 8 October 2015. <http://www.scidev.net/global/governance/news/chemical-weapons-convention-fails-to-address-key-issues.html>.
- “Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction.” Accessed 8 October 2015. <http://disarmament.un.org/treaties/t/cwc/text>.
- “DNA Nanobots Set To Seek and Destroy Cancer Cells In Human Trial | IFLScience.” Accessed 8 October 2015. <http://www.iflscience.com/health-and-medicine/dna-nanobots-will-seek-and-destroy-cancer-cells>.
- “Drones in the Defense Budget.” Center for the Study of the Drone. Accessed 8 October 2015. <http://dronecenter.bard.edu/drones-in-the-defense-budget/>.
- Fang, Jian-Shuen, Qi Hao, David J. Brady, Mohan Shankar, Bob D. Guenther, Nikos P. Pitsianis, and Ken Y. Hsu. “Path-Dependent Human Identification Using a Pyroelectric Infrared Sensor and Fresnel Lens Arrays.” *Optics Express* 14, no. 2 (2006): 609. doi:10.1364/OPEX.14.000609.
- “Here’s What The Future Of Insect And Nano Drones Looks Like [VIDEO].” *International Business Times*. Accessed 6 October 2015. <http://www.ibtimes.com/heres-what-future-insect-nano-drones-looks-video-1532592>.
- Huber, Arthur F. II, Lt Col. *Death by a Thousand Cuts: Micro-Air Vehicles in the Service of Air Force Missions*. Occasional Paper 29. Maxwell AFB, AL: Air University, 2002.
- “In New Mass-Production Technique, Robotic Insects Spring to Life | Harvard John A. Paulson School of Engineering and Applied Sciences.” Accessed 8 October 2015. <http://www.seas.harvard.edu/news/2012/02/new-mass-production-technique-robotic-insects-spring-life>.
- Jovene, Vincent T. Jr, Lt Col. *Next Generation Nanotechnology Assembly Fabrication Methods: A Trend Forecast*. Occasional Paper 64. Maxwell AFB, AL: Air University, 2008.
- Liao, Joseph C., Mitra Mastali, Vincent Gau, Marc A. Suchard, Annette K. Møller, David A. Bruckner, Jane T. Babbitt, et al. “Use of Electrochemical DNA Biosensors for Rapid

- Molecular Identification of Uropathogens in Clinical Urine Specimens.” *Journal of Clinical Microbiology* 44, no. 2 (February 1, 2006): 561–70. doi:10.1128/JCM.44.2.561-570.2006.
- “Making Viruses in the Lab Deadlier and More Able to Spread: An Accident Waiting to Happen.” *Bulletin of the Atomic Scientists*. Accessed 8 October 2015. <http://thebulletin.org/making-viruses-lab-deadlier-and-more-able-spread-accident-waiting-happen7374>.
- “Materials for 3D Electronics Printing.” *Voxel8: 3D Electronics Printing*. Accessed 8 October 2015. <http://www.voxel8.co/materials/>.
- “New Life: Scientists Create First Semi-Synthetic Organism with ‘Alien’ DNA | Science | News | The Independent.” Accessed 8 October 2015. <http://www.independent.co.uk/news/science/new-life-scientists-create-first-semi-synthetic-organism-9333371.html>.
- O’Connor, Mary Catherine. “Here Come the Swarming Drones.” *The Atlantic*, October 31, 2014. <http://www.theatlantic.com/technology/archive/2014/10/here-come-the-swarming-drones/382187/>.
- “Press Releases: AV Develops World’s First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA - AeroVironment, Inc.” Accessed 8 October 2015. [http://www.avinc.com/resources/press\\_release/aerovironment\\_develops\\_worlds\\_first\\_fully\\_operational\\_life-size\\_hummingbird](http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird).
- “Raspberry Pi 2 Model B.” *Raspberry Pi*. Accessed 8 October 2015. <https://www.raspberrypi.org/products/raspberry-pi-2-model-b/>.
- “Robobees.” Accessed 8 October 2015. <http://robobees.seas.harvard.edu/>.
- “The Past and the Future of Drones | Tumotech.” Accessed 8 October 2015. <http://www.tumotech.com/2014/06/17/the-past-and-the-future-of-drones/>.
- “UNODA - The Biological Weapons Convention.” Accessed 8 October 2015. <http://www.un.org/disarmament/WMD/Bio/>.
- Yost, Peter. “Nova: Rise of the Drones,” *PBS Video*. 53 min., 2013. <http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html>